UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,767	03/16/2006	Roberto Avanzi	DE030202US1	5670

65913 7590 04/16/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
04/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/559,767	AVANZI, ROBERTO	
	Examiner	Art Unit	
	SHEWAYE GELAGAY	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☒ Claim(s) *10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/7/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the original application filled on 12/7/05. Claims 1-10 are pending.

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 12/07/05 has been considered by the examiner (see attached PTO 1449).

Oath/Declaration

1. The Oath filed on 3/16/06 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

2. The drawings were received on 12/7/05. These drawings are accepted.

Specification

1. Applicant is asked to submit a substitute specification including proper section headings as outlined below:

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Objections

3. Claims 1-10 are objected to because of the following informalities: Claims 1-10 are method claims, however, the claims do not recite active words that would be appropriate to set forth steps taken in a method claim. Appropriate correction is required.

4. Claims 1-2 and 7 are objected to for the following reason. The claim Language must be more specific for Examiner to understand and be able to search for the invention. For example, claims 1, 2 and 7 recite "the hyperelliptic curve and/or at least

one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result" the claim as presented cause ambiguities, which make examination difficult. Examiner will interpret the claims to their broadest reasonable interpretation until claims are submitted in a more clear presentation.

5. Claim 10 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in an alternative only, cannot depend from any other multiple dependent claim. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

8. Claims 1-2, 7 and 9-10 recite the term “and/or” that renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "and/or"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d).

9. Claims 7-9 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: It is unclear how exactly the microprocessor implements the particular steps recited in claim 1. Although claims 7-9 recite "a microprocessor," the claims still do not provide any functional interrelationship to any software and hardware structural components to provide method steps of claim 1 that is processed by the microprocessor.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 1-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The cited method including steps "of a hyperelliptic curve at least one element of a first group, in particular reduced divisor

and/or at least one intermediate result of a scalar multiplication is randomized" is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. Dependent claims 2-6 do not cure the deficiencies of the independent claim, therefore, are also rejected for the same reason set forth above.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by Coron et al., "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems" 1999, pages 1-11 (hereinafter Coron).

As per claim 1:

Coron teaches a method for defence against at least one attack made by means of differential power analysis in at least one hyperelliptic cryptosystem, in particular in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, characterised in that the hyperelliptic curve and/or at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication is

randomised. (*5. Countermeasures Against DPA; introducing random numbers during the computation of Q=dP; 5.3 randomized projective coordinates...randomizing the projective coordinate representation of a point P=(X,Y,Z). Before each new execution of the scalar multiplication algorithm for computing Q=dP, the projective coordinates of P are randomized according to equation (3) with a random λ. The randomization can also occur after each point addition and doubling*)

As per claim 2:

Coron teaches all the subject matter as discussed above. In addition, Coron further teaches that the bits of the operand to be processed and/or encoded in the hyperelliptic cryptosystem are represented by the hyperelliptic curve, in particular by at least one co-efficient of the hyperelliptic curve, and/or by at least one base element of the cryptosystem, such as by at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication. (*5. Countermeasures Against DPA; introducing random numbers during the computation of Q=dP; 5.3 randomized projective coordinates. Before each new execution of the scalar multiplication algorithm for computing Q=dP, the projective coordinates of P are randomized according to equation (3) with a random λ. The randomization can also occur after each point addition and doubling*)

As per claim 3:

Coron teaches all the subject matter as discussed above. In addition, Coron further teaches that at least one scalar multiplication in the Jacobian variation of the hyperelliptic curve takes place in a second group different from the first group and

isomorphic in relation to the first group, in particular selected at random. (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*)

As per claim 4:

Coron teaches all the subject matter as discussed above. In addition, Coron further teaches the following steps:

transformation of the Jacobian variation of the hyperelliptic curve by means of at least one depiction, in particular by means of at least one K-isomorphism, into the Jacobian variation of the transformed hyperelliptic curve; (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*)

multiplication of the Jacobian variation of the transformed hyperelliptic curve with at least one scalar; (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*) and

back transformation of the Jacobian variation multiplied by the scalar (n) of the transformed hyperelliptic curve by means of the depiction inverse to the depiction in a Jacobian variations of the hyperelliptic curve multiplied by scalars,

where

the depiction corresponds to the transition from the first group to the second group

the inverse depiction corresponds to the transition from the second group to the first group. (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*)

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Coron et al., "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems" 1999, pages 1-11 (hereinafter Coron) in view of Lange "Weighted Coordinates on Genus 2 Hyperelliptic Curves" October 11, 2002, pages 1-20.

As per claim 5:

Coron teaches all the subject matter as discussed above. Coron does not explicitly disclose the steps: depiction of at least one in particular reduced divisor with associated polynomial pair as at least one quintuplet in projective co-ordinates, where U(t)=t.sup.2+U.sub.1t/Z+U.sub.0/Z and V(t)=V.sub.1t/Z+V.sub.0/Z; selection, in particular random selection, of at least one non-vanishing element from the field; and conversion of the quintuplet by means of a selected element into the converted

quintuplet. Lange in analogous art, however, further discloses the steps: depiction of at least one in particular reduced divisor with associated polynomial pair as at least one quintuplet in projective co-ordinates, where U(t)=t.sup.2+U.sub.1t/Z+U.sub.0/Z and V(t)=V.sub.1t/Z+V.sub.0/Z; selection, in particular random selection, of at least one non-vanishing element from the field; and conversion of the quintuplet by means of a selected element into the converted quintuplet. (*pages 2-3; 2. The New System of Coordinates; coordinates one lets [U1U0V1V0Z stand for X^2+U1/Zx+U0/Z and V1/Zx+V0/Z*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron with Lange in order to obtain inversion free formulae that are faster than projective by considering weighted coordinates. (Abstract; Lange)

As per claim 6:

Coron teaches all the subject matter as discussed above. Coron does not explicitly disclose the following steps: depiction of at least one in particular reduced divisor with associated polynomial pair as at least one sextuplet a projective co-ordinates, where U(t)=t.sup.2+U.sub.1t/Z.sub.1.sup.2+U.sub.0/Z.sub.1.sup.2 and V(t)=V.sub.1t/(Z.sub.1.sup.3Z.sup.2)+V.sub.0/(Z.sub.1.sup.3Z.sub.2); selection, in particular random selection, of at least two non-vanishing elements from the field; and conversion of the sextuplet by means of a selected elements into the converted sextuple. Lange in analogous art, however, further discloses the following steps: depiction of at least one in particular reduced divisor with associated polynomial pair as at least one sextuplet a projective co-ordinates, where

U(t)=t.sup.2+U.sub.1t/Z.sub.1.sup.2+U.sub.0/Z.sub.1.sup.2 and V(t)=V.sub.1t/(Z.sub.1.sup.3Z.sup.2)+V.sub.0/(Z.sub.1.sup.3Z.sub.2); selection, in particular random selection, of at least two non-vanishing elements from the field; and conversion of the sextuplet by means of a selected elements into the converted sextuple. (*pages 2-3; 2. The New System of Coordinates; let [U1,U0,V1,V0,Z1,Z2] correspond to affine point [X^2+U1/Z^2x+u0/z^21, V1/z^3Z2x+V0/Z^3iZ2]*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron with Lange in order to obtain inversion free formulae that are faster than projective by considering weighted coordinates. (Abstract; Lange)

16. Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Coron et al., "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems" 1999, pages 1-11 (hereinafter Coron) in view of Okeya et al. (hereinafter Okeya) US 2003/0059042.

As per claim 7:

Coron teaches all the subject matter as discussed above. Coron does not explicitly disclose a method implemented on at least one microprocessor in particular allocated to at least one chip card and/or in particular to at least one smart card. Okeya in analogous art, however, discloses a method implemented on at least one microprocessor in particular allocated to at least one chip card and/or in particular to at least one smart card. (*figure 6, item 701; paragraph [164-170]*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to

modify the method disclosed by Coron with Okeya in order to safeguard against side channel attack and further carry out the processing at high speed. (paragraph [187]; Okeya)

As per claim 8:

Coron teaches all the subject matter as discussed above. Coron does not explicitly disclose a microprocessor working according to a method as claimed in claim 1.Okeya in analogues art, however, discloses a microprocessor working according to a method as claimed in claim 1. (*figure 6, item 701; paragraph [164-170]*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron with Okeya in order to safeguard against side channel attack and further carry out the processing at high speed. (paragraph [187]; Okeya)

As per claim 9:

Coron teaches all the subject matter as discussed above. Coron does not explicitly disclose a device, in particular a chip card and/or in particular a smart card, with at least one microprocessor as claimed in claim 8. Okeya in analogus art, however discloses a device, in particular a chip card and/or in particular a smart card, with at least one microprocessor as claimed in claim 8. (*figure 6, item 701; paragraph [164-170])* Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron with Okeya in order to safeguard against side channel attack and further carry out the processing at high

speed. (paragraph [187]; Okeya)

Claim Rejections - 35 USC § 102

17. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

18. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Joye et al., "Protections against Differential Analysis for Elliptic Curve Cryptography" Springer-Verlag, 2001, pages 1-15 (hereinafter Joyce).

As per claim 1:

Joyce teaches a method for defence against at least one attack made by means of differential power analysis in at least one hyperelliptic cryptosystem, in particular in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, characterised in that the hyperelliptic curve and/or at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication is randomised. (*4. Randomizing the Basepoint*)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. G./
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437